



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/690,017	10/21/2003	James P. Goddard	END920030107US1	4833
26502 7590 05/12/2009				
IBM CORPORATION				
IPLAW SHCB/40-3				
1701 NORTH STREET				
ENDICOTT, NY 13760				
EXAMINER				
HOANG, DANIEL L				
ART UNIT		PAPER NUMBER		
2436				
NOTIFICATION DATE		DELIVERY MODE		
05/12/2009		ELECTRONIC		

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

endiplay@us.ibm.com

### Office Action Summary

**Application No.**

10/690,017

**Applicant(s)**

GODDARD, JAMES P.

**Examiner**

DANIEL L. HOANG

**Art Unit**

2436

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 13 January 2009.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1,3,7-10,12,15,19,20 and 25-37 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1,3,7-10,12,15,19,20 and 25-37 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

### **DETAILED ACTION**

In view of the Appeal Brief filed on 9/02/08, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

- (1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,
- (2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

### ***Response to Arguments***

Applicant's arguments with respect to amended claim 1 have been considered but are moot in view of the new ground(s) of rejection. The remaining new and amended claims are addressed below.

### **CLAIMS PRESENTED**

Claims 1, 3, 7-10, 14-15, 19, and 25-37 are presented.

### **CLAIM REJECTIONS**

***Claim Rejections - 35 USC § 103***

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. **Claims 1, 3, 7-10, 14-15, 19, and 25-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Townsend (US Patent No. 6374358), and further in view of Wilkinson (US Patent No. 7007026).**

**As per claims 1, 25, and 32:**

A computer implemented method for evaluating a security risk of an application, said method comprising the steps of:

*[see col. 2, lines 19-23, wherein Townsend teaches systems and methods that create a security model for an organization operating an application on a computer network to protect the application from attack by unauthorized resources.]*

~~determining whether the application is shared by different customers;~~

~~*[see col. 4, lines 20-37, wherein Townsend teaches rules for identifying conditions that may require increasing existing countermeasure strengths, said rules including number of employees, users, computers, and connections. These rules are used to calculate the appropriate countermeasure strength level. As the Townsend reference is related to selecting a security model for an organization operating an application on the organization's computer network, it is clear that the rules cited above are used to calculate the impact that an amount of users will have on an application operating on the organization's computer network. Examiner is interpreting the users cited in the Townsend reference as being analogous to the claimed "customers".]*~~

~~determining whether a third party can have unauthorized administrative authority to data maintained by said application;~~

~~*[see col. 3, 17-33, wherein Townsend teaches the organization determines types of attacks that it is subject to and the corresponding countermeasures. The types of attacks include, "unauthorized access to and use of confidential business information". The fact*~~

*that the data is confidential is enough to say that access to such data would require administrative authority. Being that the access is unauthorized clearly denotes the access is initiated by an unauthorized third party.*

determining whether a third party can have unauthorized read and/or write access to data maintained by said application;

*[see col. 3, lines 23-24, "unauthorized modification of data records"]*

assigning a numerical value or weight to each of the foregoing determinations, each of said numerical values or weights corresponding to a significance of the respective determination in evaluating security risk; and combining said numerical values or weights to evaluate security risk.

*[see col. 4, lines 1-52, wherein the rule databases may be constructed as rules for use in determining current and recommended countermeasure strength levels. Rule base A reduces the user input on a questionnaire to a numeric value indicating the current countermeasure strength level.]*

While examiner does not agree with applicant's assessment that Townsend does not recite the limitation of "determining whether the application is shared by different customers", for sake of prosecution it is presumed that Townsend is mute in teaching this limitation. Thus the Wilkinson reference is relied upon.

Wilkinson teaches a method for controlling access to localized application values to applications (see col. 2, lines 49-67). These application values include user roles indicating data access levels for users of the application. Users with administrative access will clearly have a higher access level than users without administrative access to the application. It would be obvious to one of ordinary skill in the art to modify the invention taught by Townsend to include a step wherein it is determined whether the application has differing levels of access as taught by Wilkinson. It would be advantageous to do so because such a determination would result in a higher risk if the application has different access levels. It is possible that data maintained by a user with administrative access levels may be accessed by a user without said administrative access levels.

**As per claim 3:**

A computer implemented method as set forth in claim 1 further comprising the steps of: determining whether said application is subject to industry controls for security; and assigning a numerical value or weight to the determination whether said application is subject to industry controls for security, and using the numerical value or weight for the determination whether said application is subject to industry controls for security in evaluation security risk.

*[see col. 2, lines 9-15, "industry practices"]*

**As per claim 7:**

A computer implemented method as set forth in claim 1 further comprising the steps of: determining whether a third party can have unauthorized read and write access to said data; and assigning a numerical value or weight to the determination whether a third party can have unauthorized read and write access to said data, and using the numerical value or weight for the determination whether a third party can have unauthorized read and write access to said data in evaluating said security risk.

*[see rejection of claim 1]*

**As per claim 8, 27:**

A computer implemented method as set forth in claim 1 further comprising the steps of: determining whether a vulnerability in said application can be exploited by a person or program which has not been authenticated to said application or a system in which said application runs; and assigning a numerical value or weight to the determination whether the vulnerability in said application can be exploited by a person or program which has not been authenticated to said application or a system in which said application runs and using the numerical value or weight for the determination whether a third party can have unauthorized read and write access to said data in evaluating said security risk.

*[see col. 3, lines 21-24]*

**As per claim 9:**

A computer implemented method as set forth in claim 1 further comprising the steps of:  
determining whether data maintained by or accessed by said application is confidential; and wherein the numerical value or weight assigned to the determination whether a third party can have unauthorized access to said data is based in part on whether said data is confidential.

*[see col. 3, lines 21-22]*

**As per claim 10, 28, 34:**

A method as set forth in claim 1 further comprising the steps of:  
determining whether a customer has direct use of said application; and assigning a numerical value or weight to the determination whether a customer has direct use of said application, and using the numerical value or weight for the determination whether a customer has direct use of said application in evaluating said security risk.

*Townsend does not explicitly cite direct use of an application as an attack. Townsend cites that attack and countermeasure types may vary depending on the application being evaluated (see col. 3, lines 30-33). Examiner contends that a customer that is able to have direct use of the application is an obvious potential attack on the system. Therefore, it would have been obvious at the time of the invention to evaluate the security risk of the application by determining whether a customer has direct use of the application.*

**As per claim 12:**

A computer implemented method as set forth in claim 1 further comprising the steps of:  
determining whether there is an intrusion detection system and vulnerability scanning for said application; and assigning a numerical value or weight to the determination whether there is an intrusion detection system and vulnerability scanning for said application, and using the numerical value or weight for the determination whether a customer has direct use of said application in evaluating said security risk.

*[see col. 3, lines 26-29, "password protection, event logging, authentication"]*

**As per claim 19, 30, 36:**

A computer implemented method as set forth in claim 1 further comprising the step of comparing the evaluation of said security risk to a cost savings provided by said application, and determining whether to certify said application for use based in part on said comparison.

*[see col. 4, lines 53-66]*

**As per claim 20, 31, 37:**

A computer implemented method as set forth in claim 1 further comprising the step of comparing the evaluation of said security risk to a revenue provided by said application, and determining whether to certify said application for use based in part on said comparison.

*[see col. 7, lines 1-12]*

3. Claims 15, 29, and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Townsend and Wilkinson as applied to claim 1 above, and further in view of Minemura, US PGP No. 20030114144.

**As per claim 15, 29, 35:**

A computer implemented method as set forth in claim 1 further comprising the steps:  
determining whether there is a requirement for authentication of said application or a system in which said application runs to other systems before connection of said application or said system in which said application runs to said other systems; and assigning a numerical value or weight to the determination whether there is a requirement for authentication of said application or a system in which said application runs to other systems before connection of said application or said system in which said application runs to said other systems, and using the numerical value or weight for said requirement for authentication in evaluating said security risk.



Townsend and Wilkinson have been discussed above. The combination of Townsend and Wilkinson are mute in teaching application authentication as a requirement evaluating security risk. The Minemura reference is relied upon for this limitation.

Minemura teaches an application authentication system (see paragraphs 013-015). It would be obvious to one of ordinary skill in the art to modify the Townsend reference to include the application authentication system taught by Minemura because application security is a security risk. It is possible that the application may be used to perform an invalid operation. Authenticating the application is a possible way of thwarting such attempts. Determining whether the application is required to authenticate would clearly make the system more secure and allow it to better evaluate an application's security risk.

### ***Conclusion***

3. Any response to this Office Action should be **faxed to (571) 273-8300 or mailed to:**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**Hand-delivered responses** should be brought to

Customer Service Window  
Randolph Building  
401 Dulany Street  
Alexandria, VA 22314

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel L. Hoang whose telephone number is 571-270-1019. The examiner can normally be reached on Monday - Thursday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached at (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2436

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Daniel L. Hoang/  
Examiner, Art Unit 2436

/Nasser G Moazzami/  
Supervisory Patent Examiner, Art Unit 2436